

**RICHMOND POLICE DEPARTMENT GENERAL ORDER**

NOTE: This directive is for internal use only, and does not enlarge an employee's civil liability in any way. It should not be construed as the creation of a higher standard of safety or case in an evidentiary sense, with respect to third party claims. Violation of this directive, if proven, can only form the basis of a complaint by this Department, and then only in a non-judicial administrative setting.

Chapter 7	Number 27	Effective Date 11/10/09	Review Date 2012
Subject COMPUTER FORENSIC PROCEDURES			☐ New Order ☒ Replaces G.O. 7-27 (05/26/06)
References CALEA 83.2.5, 83.2.6, 84.1.1a., b. VLEPSC ADM.16.01a, ADM.16.02a General Order 3-12, Handling Property and Evidence			
			11/10/09
Chief of Police or Designee			Date

I. PURPOSE

The purpose of this policy is to facilitate the identification, investigation and prosecution of persons who utilize computers in the furtherance of criminal activity.

II. POLICY

It is the policy of the Richmond Police Department that, during criminal investigations, only agency designated employees that are trained in proper digital evidence handling techniques or are acting under the direction of such persons, shall seize digital evidence. In addition, the analysis of such evidence, whether done on-scene or after seizure, may only be performed by those persons designated as Computer Forensic Examiners.

III. ACCOUNTABILITY STATEMENT

All employees are expected to fully comply with the guidelines and timelines set forth in this general order. Failure to comply will result in appropriate corrective action. Responsibility rests with the Division Commander to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated.

IV. DEFINITIONS

- A. Computer Forensic Examiner – **An authorized** sworn or civilian member of the Richmond Police Department trained in the techniques of computer data recovery and seizure.
- B. Digital Evidence – **Computers, cell phones**, hard-drives, thumb-drives, compact-discs, floppy-disks, smart-cards, tape-media or other devices designed to hold data in digital format.

- C. Digital Evidence Collection Specialist – ***An authorized*** sworn or civilian member of the Richmond Police Department trained in the collection of digital evidence.
- D. Digital Information Processing Machines – Computers, personal digital assistants (PDAs), MP3 players, digital cameras or other devices designed to interpret or manipulate information stored in digital format ***on*** devices such as those listed under “Digital Evidence” above.

V. PROCEDURE

This policy shall apply only in those cases where data residing on computer systems, ***cell phones***, recording devices and/or ***other storage*** media are being sought as evidence in an investigation.

A. Seizure:

1. ***It is the responsibility of the officer or investigator on-scene to notify his/her immediate supervisor in situations where handling digital media is required.***
2. No Department member, except those designated employees who are properly trained in handling digital evidence or who are acting under the direction of such employees, shall power-off, disconnect, power-on or access a computer system, ***cell phone***, recording device or ***other type of storage*** media that is to be seized.
3. When it is determined that digital evidence is to be seized and processed and neither an examiner nor collection specialist is available, ***the supervisor*** shall contact the on-call forensic examiner ***and request him/her to respond on-scene.*** Investigators who have computer systems as targets in their search warrants shall notify the Officer-In-Charge of the ***Financial and Computer Crimes Unit*** 24 hours prior to the execution of the warrant ***to ensure that*** a computer forensic examiner will respond to the target ***location*** and assist in the safe collection of the system.
4. Any questions regarding equipment seizure (wording of search warrants, etc.) can be addressed by contacting the ***Financial and Computer Crimes Unit*** during normal business hours or by contacting the ***Department of Emergency Communications (DEC)*** during non-business hours. Inquiries to the ***DEC*** will be directed to the on-call investigator.

B. Transport:

1. The computer forensic examiner or digital evidence collection specialist tasked with the seizure in question will handle the transportation of the seized equipment unless other approved arrangements are made. A qualified computer forensic examiner or digital collection specialist must give approval in these instances.
2. If a computer forensic examiner or evidence collection specialist is unable to physically assist in the transportation of the seized items, ***the sworn officer or on-scene investigator must adhere to*** the following:
 - a) All items ***shall*** be packaged in a manner suitable for safe/secure transport;

- b) All items shall be labeled so they are readily identifiable; and,
 - c) At no time ***shall*** items be placed on or near devices that produce strong magnetic fields, i.e. radio equipment, etc.
3. ***If the device to be transported is a cell phone, the following procedures must be followed:***
- a) ***If the phone is “ON,” it shall be isolated from the network in one of the following ways:***
 - (1) ***Place the phone in “Airplane,” “Flight” or “Stand-Alone” mode.***
 - (2) ***Power the device off.***
 - (3) ***Utilize a signal blocking device such as a Faraday™ bag or arson can. (WARNING: This will cause the battery to expire rapidly.)***
 - b) ***If the phone is “OFF,” leave it in the off mode.***

C. Storage:

- 1. All computer evidence seized for purposes of analysis must be transported to the Property and Evidence Unit, logged into agency records and placed under the control of Property and Evidence Unit prior to the end of ***the assigned member’s*** tour-of-duty.
- 2. Once ***the items have been logged*** into the system, a computer forensic examiner or digital evidence collection specialist will transport the items to the computer forensic lab where they will be stored in an approved area until analysis is complete.

D. Analysis, Reviews and Examinations:

All requests for reviews, examinations and analysis must include a copy of the search warrant or signed consent form ***and a Request for Forensic Examination (PD-55)*** before a computer forensic examiner can take any action. The time frame for completion will depend on the volume of materials seized in combination with the reason for seizure. Reasons for seizure will generally fall within one of the following categories:

- 1. Reviews – The most unobtrusive investigations ***that*** generally involve an overall look at the system type, size and operating system. ***Reviews*** are often done for the purposes of determining the existence of such things as pornography or Internet access to unauthorized sites. As stated above, they may also be done to determine ownership on lost and found or stolen property.
- 2. Examinations – Normally done in an effort to locate a ***particular*** file or text statement involving a specific crime or activity which is known or highly suspected to exist on the media ***device*** in question.

3. Analysis – Involves a complete and detailed review of the submitted media *device*. This is the most obtrusive investigation and will generally take the longest period of time to complete.

E. Dissemination:

Upon completion of *the* analysis, *review or examination*, the computer forensics *examiner* will:

1. Send a report of the findings to the requesting officer.
2. *Maintain* a copy of the findings *in* the *Financial and Computer Crimes* Unit.

F. Disposition:

1. Final dispositions or destruction of evidence shall be done in accordance with *General Order 3-12, Handling Property and Evidence* or, when applicable, at the discretion of the court.
2. Evidence released by the court shall be returned to the owner as soon as practical.

VI. ROLES AND ACCOUNTABILITY

A. *Computer Forensic Examiner shall:*

1. *Recover, collect and analyze computer evidence either on-scene or post-seizure;*
2. *Respond on-scene and assist in safe collections when evidence is to be seized and a collection specialist is not available;*
3. *Give approval in instances where arrangements for transport of seized equipment is tasked to someone other than him/herself or the digital evidence collection specialist;*
4. *Log seized items into the Property & Evidence Unit prior to end of tour-of-duty;*
5. *Transport seized equipment into computer lab following log-in;*
6. *Ensure that if a seized cell phone is “ON,” it is isolated from the network by being placed in the “Airplane,” “Flight” or “Stand-Alone” mode, powered off and a blocking device such as a Faraday™ Bag or arson can is utilized;*
7. *Ensure that if a seized cell phone is “OFF,” it remains in this mode;*
8. *Review, examine and analyze seized material upon receipt of a completed PD-55;*
9. *Send report of finding to the requesting officer or investigator; and,*
10. *Maintain a copy of finding in the Financial and Computer Crimes Unit.*

B. *Digital Evidence Collection Specialist shall:*

1. *Assist in the collection and transportation of seized equipment;*
2. *Give approval in instances where arrangements for transport of seized equipment is tasked to someone other than him/herself or the computer forensic examiner;*
3. *Log seized equipment into the Property & Evidence Unit prior to the end of tour-of-duty;*
4. *Transport seized equipment into computer lab following log-in;*
5. *Ensure that if a seized cell phone is "ON", it is isolated from the network by being placed in the "Airplane," "Flight" or "Stand-Alone" mode, powered off and a blocking device such as a Faraday Bag or arson can is utilized; and,*
6. *Ensure that if a seized cell phone is "OFF," it remains in this mode.*

C. *Financial and Computer Crimes Unit Officer-In-Charge or designee shall:*

1. *Ensure that a computer forensic examiner will respond to the target location when notified by a sworn officer who is in possession of a search warrant targeting a computer system; and,*
2. *During normal business hours, address questions regarding equipment seizure.*

D. *Sworn Officer/Investigator shall:*

1. *Assist in the transportation of seized items if the computer forensic examiner or digital evidence computer specialist is unable to physically assist;*
2. *Log items into the Property & Evidence Unit prior to the end of tour-of-duty;*
3. *Notify the supervisor in situations where handling digital media is required;*
4. *Notify the Financial & Computer Crimes Unit 24 hours prior to the execution of a search warrant if computer systems are listed as a target in the warrant;*
5. *Prior to the execution of a search warrant which may involve digital media, make arrangements to have a staff-person, trained in proper handling techniques, available on-scene;*
6. *Ensure that seized items are securely packaged for transport;*
7. *Ensure that seized items are labeled and readily identifiable;*
8. *Ensure that seized items are not placed near devices producing a strong magnetic field;*
9. *Ensure that seized cell phones which are "ON" are isolated from the network using a Faraday™ bag or arson can; and,*

10. *Ensure that seized cell phones which are “OFF” remain in this mode.*

E. *Supervisor shall:*

When neither an examiner or collection specialist is available, contact the on-call forensic examiner to request that he/she responds on-scene;

F. *Department of Emergency Communications shall:*

During non-business hours, direct inquiries regarding the seizure of digital equipment to the on-call investigator.

VII. FORMS

A. Consent Form

B. PD-55, Request for Forensic Examination